WHAT IS CLAIMED IS:

1. An encryption level indicator calculation method based on an encryption processing algorithm and composed of:

a step of setting a common key block encryption processing algorithm, which is to serve as said encryption processing algorithm to be used as the base of said encryption level indicator calculation method, has a key-scheduling part comprising a linear transformation part and a non-linear transformation part and includes:

a sub-step of generating initial values U_i (where i = 1, 2 and so on) from a master key;

a sub-step of calculating intermediate values $Z_i^{(0)}$ (where i = 1, 2 and so on) from said initial values U_i (where i = 1, 2 and so on);

a plurality of sub-steps of calculating intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on) from intermediate values $Z_i^{(r-1)}$ (where i = 1, 2 and so on);

a sub-step of calculating said non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) from said intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) and said initial values U_i (where i = 1, 2 and so on); and

a sub-step of calculating round keys $K_i^{(r)}$ (where i

= 1, 2 and so on and r = 1, 2 and so on) from said intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) and said non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on);

a step of eliminating said intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) serving as variables so that said round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) can be expressed as a linear combination of said initial values U_i (where i = 1, 2 and so on) and said non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on);

a step of transforming said linear combination into a simultaneous linear equation completing transposition of terms and, thus, consisting of only terms of said initial values U_i (where i = 1, 2 and so on) and said non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) on the right-hand side of said equation;

a step of transforming said simultaneous linear equation into a matricial equation;

a step of multiplying both the left-hand and right-hand sides of said matricial equation by a row-deform

unitary matrix deforming a matrix on the right-hand side of said matricial equation obtained as a result of transformation into a step matrix from the left;

a step of creating a new matrix consisting of lowest N rows of a matrix on the left-hand side of said matricial equation obtained as a result of transformation where N is a number obtained as a result of subtracting the rank value of said step matrix from the number of rows in said step matrix; and

a step of finding N linear-relation equations by multiplying a column vector consisting of said round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) as elements by said new matrix generated at said preceding step,

where:

symbol U_i (where i = 1, 2 and so on) denotes an initial value of said key-scheduling part;

symbol $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an intermediate value of said key-scheduling part;

symbol $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an output of said non-linear transformation part; and

symbol $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2

and so on) denotes a round key calculated from said intermediate values Z_i (where i = 1, 2 and so on).

2. A program to be executed as a computer program in carrying out an encryption level indicator calculation process based on an encryption processing algorithm and composed of:

a step of setting a common key block encryption processing algorithm, which is to serve as said encryption processing algorithm to be used as the base of said encryption level indicator calculation process and includes:

a sub-step of generating initial values U_i (where i = 1, 2 and so on) from a master key;

a sub-step of calculating intermediate values $Z_i^{(0)}$ (where i = 1, 2 and so on) from said initial values U_i (where i = 1, 2 and so on);

a plurality of sub-steps of calculating intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on) from intermediate values $Z_i^{(r-1)}$ (where i = 1, 2 and so on);

a sub-step of calculating said non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) from said intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) and said initial values U_i (where i = 1, 2 and so on); and

a sub-step of calculating round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) from said intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) and said non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on);

a step of eliminating said intermediate values $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) serving as variables so that said round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) can be expressed as a linear combination of said initial values U_i (where i = 1, 2 and so on) and said non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on);

a step of transforming said linear combination into a simultaneous linear equation completing transposition of terms and, thus, consisting of only terms of said initial values U_i (where i = 1, 2 and so on) and said non-linear transformation part outputs $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) on the right-hand side of said equation;

a step of transforming said simultaneous linear equation into a matricial equation;

a step of multiplying both the left-hand and right-

hand sides of said matricial equation by a row-deform unitary matrix deforming a matrix on the right-hand side of said matricial equation obtained as a result of transformation into a step matrix from the left;

a step of creating a new matrix consisting of lowest N rows of a matrix on the left-hand side of said matricial equation obtained as a result of transformation where N is a number obtained as a result of subtracting the rank value of said step matrix from the number of rows in said step matrix; and

a step of finding N linear-relation equations by multiplying a column vector consisting of said round keys $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) as elements by said new matrix generated at said preceding step,

where:

symbol U_i (where i = 1, 2 and so on) denotes an initial value of said key-scheduling part;

symbol $Z_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an intermediate value of said key-scheduling part;

symbol $V_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes an output of said non-linear transformation part; and

symbol $K_i^{(r)}$ (where i = 1, 2 and so on and r = 1, 2 and so on) denotes a round key calculated from said intermediate values Z_i (where i = 1, 2 and so on).